



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.3948

(06/2011)

SERIES Q: SWITCHING AND SIGNALLING
Signalling requirements and protocols for the NGN –
Testing for NGN networks

Service testing framework for VoIP at NGN UNI

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Draft Recommendation ITU-T Q.3948

Service testing framework for VoIP at NGN UNI

TABLE OF CONTENTS

1.	Scope	3
2.	References	3
3.	Definitions	4
4.	Abbreviations	4
5.	Conventions	4
6.	Preparation for Testing	4
6.1.	Test object	4
6.2.	Target interface	5
6.3.	Target Recommendation	6
6.4.	Physical configuration	6
6.5.	Test scenarios of Network Integration Test (NIT)	7
6.5.1.	Test items	7
6.5.2.	Execution flow	8
6.6.	Test scenario of VoIP interoperability testing of the End-to-End service	21
6.6.1.	Test items	21
7.	Analyze the test output	23
7.1.	Test report production	23

Summary

This Recommendation describes the procedure, requirements, physical configuration and standard document sets for service testing framework for VoIP at UNI of NGN.

Keywords

VoIP, Service testing, NGN, UNI

Introduction

The World Telecommunication Standardization Assembly (WTSA-08) approved the Res.76 “Studies related to conformance and interoperability testing, assistance to developing countries, and a possible future ITU Mark programme (Johannesburg, 2008)” and assigned to all study Group with the responsibility to develop conformance and interoperability Recommendations to improve the interoperability of NGN. This Recommendation provides the test specifications framework to assure the interoperability of VoIP service at UNI of NGN. This Recommendation encourages supporting the testing of NGN in the multi vendors environments.

1. Scope

This Recommendation describes the procedure, requirements, physical configuration and standard document sets for service testing framework for VoIP at UNI of NGN. Other service tests are for further study. The purpose of this Recommendation is to describe the service testing framework for VoIP at UNI for NGN in order to confirm the conformity to the relevant ITU-T Recommendation and assure the interoperability of the NGN products at the specific interface.

2. References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T G.711] Recommendation ITU-T G.711 (1984), Pulse Code Modulation (PCM) of Voice Frequencies
- [ITU-T H.264] Recommendation ITU-T H.264 (2009), ADVANCED VIDEO CODING FOR GENERIC AUDIOVISUAL SERVICES
- [ITU-T Q.3402] Recommendation ITU-T Q.3402 (2008), NGN UNI signalling profile (Protocol set 1)
- [ISO/IEC 14496-2] ISO/IEC 14496-2 (2004), Information technology – Coding of audio-visual objects – Part 2: Visual
- [ISO/IEC 14496-3] ISO/IEC 14496-3 (2005), Information technology – Coding of audio-visual objects – Part 3: Audio
- [RFC 3016] IETF RFC 3016 (2000), RTP Payload Format for MPEG-4 Audio/Visual Streams
- [RFC 3261] IETF RFC 3261 (2002), SIP: Session Initiation Protocol
- [RFC 3262] IETF RFC 3262 (2002), Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
- [RFC 3264] IETF RFC 3264 (2002), An Offer/Answer Model with the Session Description Protocol (SDP)
- [RFC 3311] IETF RFC 3311 (2002), The Session Initiation Protocol (SIP) UPDATE Method
- [RFC 3550] IETF RFC 3550 (2003), RTP: A Transport Protocol for Real-Time Applications
- [RFC 3551] IETF RFC 3551 (2003), RTP Profile for Audio and Video Conferences with Minimal Control
- [RFC 3984] IETF RFC 3984 (2005), RTP Payload Format for H.264 Video
- [RFC 4028] IETF RFC 4028 (2005), Session Timers in the Session Initiation Protocol (SIP)
- [RFC 4566] IETF RFC 4566 (2006), SDP: Session Description Protocol

[JT-Q3402(E)] TTC JT-Q3402(E) (2011), The difference between TTC JT-Q3402 and ITU-T Q.3402 (NGN UNI Signalling Profile (Protocol Set 1))

3. Definitions

None defined in this Recommendation.

4. Abbreviations

This standard uses the following abbreviations:

MPEG	Moving Picture Experts Group
NGN	Next Generation Network
NIT	Network Integration Test
PICS	Protocol Implementation Conformance Statements
PIXIT	Protocol Implementation Extra Information for Testing
QoS	Quality of Service
RFC	Request For Comments
RTC	RTP Control Protocol
RTP	Real-Time Transport Protocol
SCF	Service Control Functions
SDP	Session Description Protocol
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
UA	User Agent
UDP	User Datagram Protocol
UNI	User-to-Network Interface
VoIP	Voice over IP

5. Conventions

None

6. Preparation for Testing

6.1. Test object

Test object of the VoIP service testing is specified with multiple Recommendations and relevant standards.

Figure 1 shows the block diagram of SIP multimedia communication terminal and yellow coloured parts are the test object of this Recommendation.

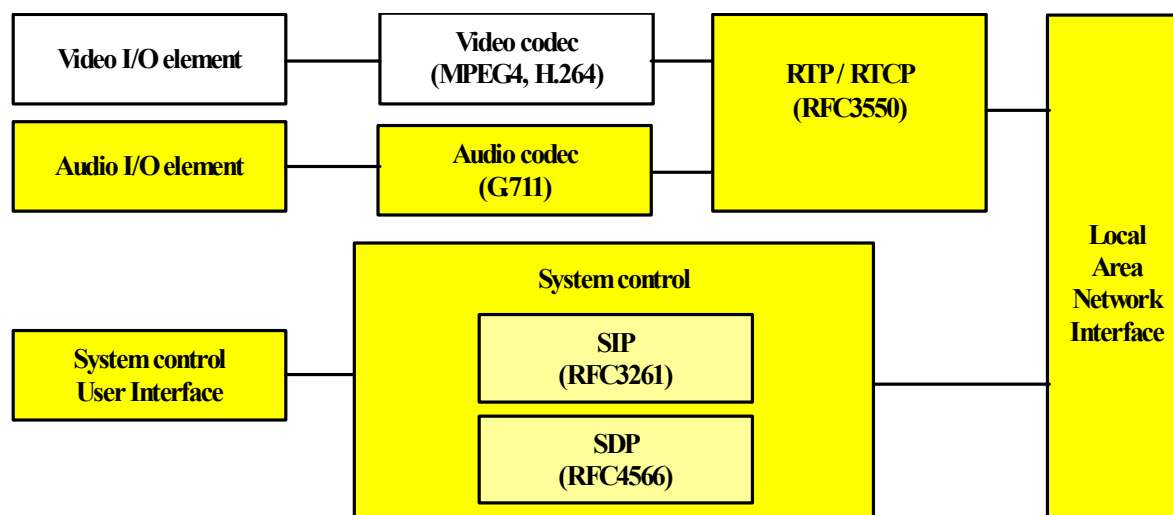


Figure 1 SIP multimedia communication terminal

Test profile should include the list of the Recommendations related to the test object of VoIP service testing.

Table 1 shows the profiles on SIP multimedia communication terminal and coloured parts are the test object of this Recommendation.

Table 1 Coding scheme and profiles

Item	VoIP	MPEG-4	H.264
Session Control	SIP (RFC3261), SDP (RFC4566)		
Capability Exchange	RFC3264	RFC3264, RFC3016	RFC3264, RFC3984
SIP extensions	RFC 3262(Reliability of provisional responses) RFC 3311(UPDATE) RFC 4028(Session Timers)		
Media Transfer	RTP (RFC3550, RFC3551), RTCP (RFC3550 Option)		
	RFC3551	Packetization mode (RFC3016)	Packetization Mode (RFC3984)
Video (High Rate:CIF, Low Rate:QCIF)	None	High:MPEG-4 Visual SP@L3 Low:MPEG-4 Visual SP@L0	High:H.264 (BP@L1.2) Low:H.264 (BP@L1)
Audio	G.711 μ /a-Law		

6.2. Target interface

UNI of the red coloured interface in figure 2 is the target interface of this Recommendation.

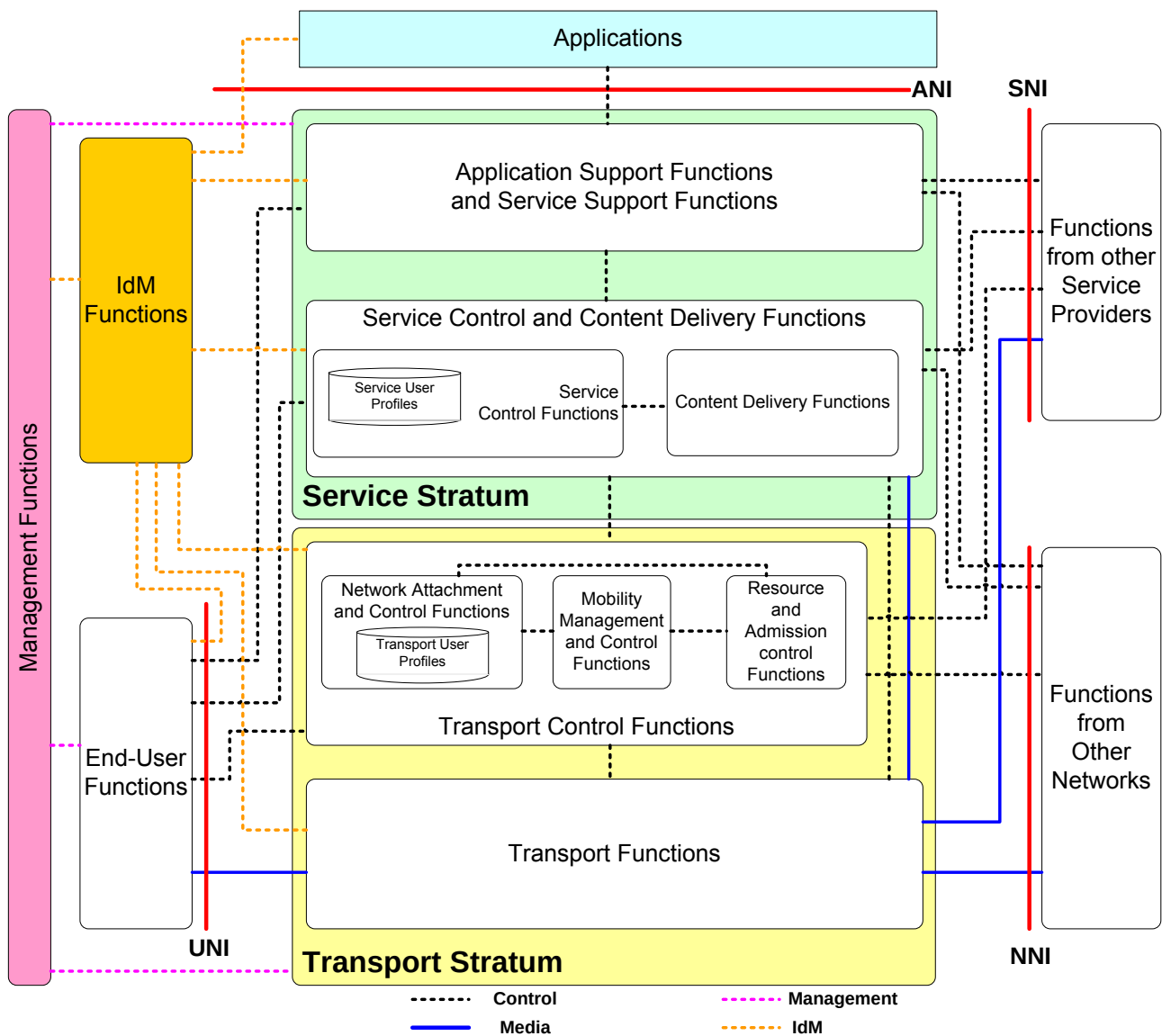


Figure2 UNI as the target interface (ITU-T Y.2012 NGN architecture overview)

6.3. Target Recommendation

ITU-T Recommendation Q.3402 NGN UNI signalling profile (Protocol set 1) is the target Recommendation.

6.4. Physical configuration

Physical configuration should define the functions which are needed for service testing. It may be depending on target protocol. This paragraph should show the items about conditions of the test configuration. There are two steps of Network Under Test (NUT), one is Network Integration Test (NIT) and the other is interoperability testing of the End-to-End service.

Figure 3 shows a sample of the general configuration of NIT for the VoIP service testing at UNI.

In this figure, the reference machine is similar to the network. And Figure 4 shows the sample of the general configuration of VoIP interoperability testing of the End-to-End service.

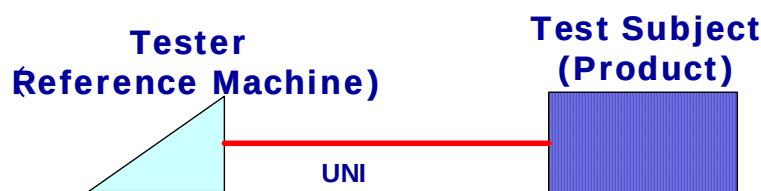


Figure 3 General Configuration of NIT for the VoIP Service testing

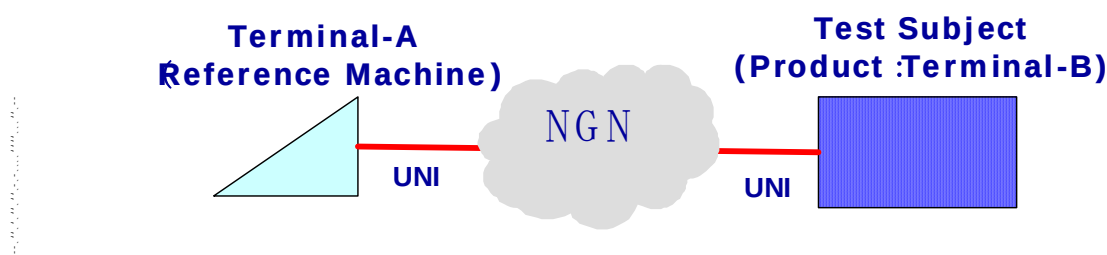


Figure 4 General Configuration of VoIP interoperability testing of the End-to-End service

6.5. Test scenarios of Network Integration Test (NIT)

The following is a sample of the Network Integration Test (NIT) for VoIP service testing at UNI.

6.5.1. Test items

Following is the sample of test items.

- A) Terminal registration
- B) Negotiating SIP capabilities
- C) Audio terminal's behaviour

For details, refer to the tables of “List of sequences.”

Table 2: List of sequences of NIT

N	Sequence Name	Corresponding clauses and figures of Annex Table p-1: List of sequences
1	Terminal registration (access-line based authentication)	Annex p.1.1
2	Deletion of terminal registration (access-line based authentication)	Annex p.1.3
3	Call origination to disconnection (IPv4, Use of <i>timer</i> and <i>100rel</i> , G.711 μ -law)	Annex p.1.4
4	Call termination to disconnection (IPv4, Use of <i>timer</i> and <i>100rel</i> , G.711 μ -law)	Annex p.1.6

- 5 Call cancellation
- 6 Busy on the terminating side

Annex p.1.7
Annex p.1.8

6.5.2. Execution flow

NGN service testing should be conducted in the following steps,

- (1) Set the test object, target interface and target Recommendations
- (2) Set the physical configuration and target products
- (3) Define the test scenarios
- (4) Examine the service testing according to the test scenarios and analyze the test output

Detail clauses are shown as follows.

6.5.2.1. Terminal registration (access-line based authentication)

This clause shows a message flow in the case that a network requires a *REGISTER* from a terminal, and access-line based terminal authentication is performed. An IPv4 address and an IPv6 address are used as *Contact address*, and *REGISTER* is performed by IPv4 UDP. The network notifies the pre-existing route by a *Service-Route* header and the available network-asserted user identity by a *P-Associated-URI* header.

In the terminal registration such as the one shown below, a SIP-URI composed of a telephone number is used as the URI to be specified in *From* header and *To* header at the time of terminal registration like the caller number shown in Annex p1.3 etc Figure 5. Note that there may be a case of using a SIP-URI which is not composed of the telephone number according to the policy of NGN carriers.

SIP domain: example1.ne.jp

TEL: 03-1111-1111, 03-1111-1112

IP (SIP): 192.0.1.1, 2001:db8:1234:5678:acde:48ff:fe01:2345

IP (SIP): 192.0.1.10, 2001:db8::1

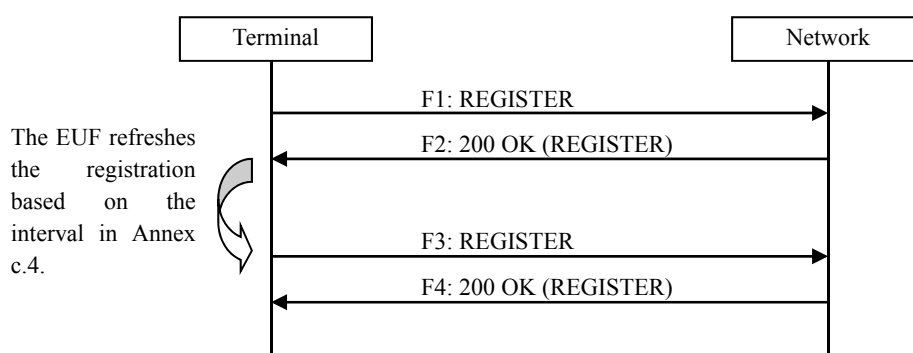


Figure 5 Terminal registration (access-line based authentication)

• F1: REGISTER

```

REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop1111111@192.0.1.1
  
```

```
CSeq: 1 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acd
e:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

- **F2: 200 OK (REGISTER)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101010
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact: <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:
1234:5678:48ff:fe01:2345]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@examp
le1.ne.jp>
Content-Length: 0
```

- **F3: REGISTER**

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acd
e:48ff:fe01:2345]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

- **F4: 200 OK (REGISTER)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:
1234:5678:48ff:fe01:2345]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@examp
```

```
le1.ne.jp>  
Content-Length: 0
```

6.5.2.2. Deletion of terminal registration (access-line based authentication)

This clause shows a message flow in the case that terminal registration is deleted under the same condition of option item selection as in Annex Table p-1 assuming that the old registration of the terminal remain in the network when the power of the terminal turns on and so on.

SIP domain: example1.ne.jp

TEL: 03-1111-1111, 03-1111-1112

IP (SIP): 192.0.1.1, 2001:db8:1234:5678:acde:48ff:fe01:2345

IP (SIP): 192.0.1.10, 2001:db8::1

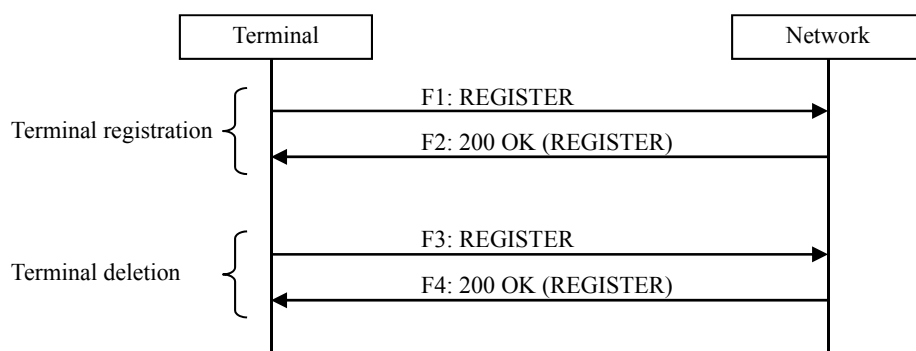


Figure 6 Deletion of terminal registration (access-line based authentication)

F1 to F2 are omitted because they are the same as those of Annex Table p-1.

▪ F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0  
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112  
Max-Forwards: 70  
To: <sip:0311111111@example1.ne.jp>  
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112  
Call-ID: qwertyuiop111111@192.0.1.1  
CSeq: 2 REGISTER  
Contact: *  
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE  
Expires: 0  
Supported: path  
Content-Length: 0
```

▪ F4: 200 OK (REGISTER)

```
SIP/2.0 200 OK  
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112  
Path: <sip:192.0.1.10;lr>  
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011  
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112  
Call-ID: qwertyuiop111111@192.0.1.1  
CSeq: 2 REGISTER  
Supported: path
```

```

Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@exam
le1.ne.jp>
Content-Length: 0

```

6.5.2.3. Call origination to disconnection (IPv4, Use of timer and 100rel, G.711 μ -law)

This clause shows a message flow of a call connection sequence on the originating side in the case that *timer* and *100rel* are enabled on both originating and terminating sides. IPv4 is used for call control signals and media, UDP is used for call control, and G.711 μ -law is used as audio media. Session refresh is performed by *UPDATE*, and disconnection (by the originating side) is finally performed by *BYE*.

This clause shows a message flow on the terminating side under the same condition of option item selections as of option item selections as Annex Table p-1.

SIP domain: example1.ne.jp
 TEL: 03-1111-1111, 03-1111-1112
 IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10
 IP (RTP): 192.0.1.11

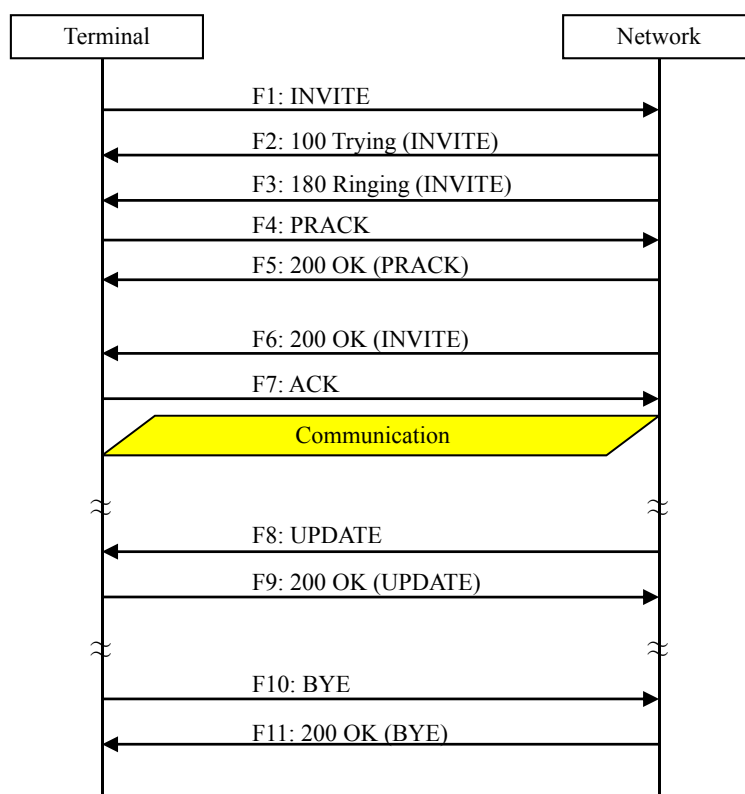


**Figure 7 Call origination to disconnection
 (IPv4, Use of timer and 100rel, G.711 μ -law) (access-line based
 authentication)**

- **F1: INVITE**

```

INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0

```

```

Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:032222222;phone-context=example1.ne.jp>
From: <sip:031111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:zxcvbnm@192.0.1.1>
P-Preferred-Identity: <sip:031111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20

```

- **F2: 100 Trying**

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:032222222;phone-context=example1.ne.jp>
From: <sip:031111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0

```

- **F3: 180 Ringing**

```

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:032222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:031111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0

```

- **F4: PRACK**

```

PRACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122

```

```
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

▪ **F5: 200 OK (PRACK)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
Content-Length: 0
```

▪ **F6: 200 OK (INVITE)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 20000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

▪ **F7: ACK**

```
ACK sip:mnbcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111123
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
```

Content-Length: 0

- **F8: UPDATE**

```
UPDATE sip:zxcvbnm@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
Max-Forwards: 64
To: <sip:031111112@example1.ne.jp>;tag=1234abcd-1111121
From: <tel:032222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:mnbcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

- **F9: 200 OK (UPDATE)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
To: <sip:031111111@example1.ne.jp>;tag=1234abcd-1111121
From: <tel:032222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:zxcvbnm@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

- **F10: BYE**

```
BYE sip:mnbcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-1111124
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:032222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:031111112@example1.ne.jp>;tag=1234abcd-1111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 3 BYE
Content-Length: 0
```

- **F11: 200 OK (BYE)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-1111124
To: <tel:032222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:031111112@example1.ne.jp>;tag=1234abcd-1111121
Call-ID: qwertyuiop111112@192.0.1.1
```

CSeq: 3 BYE
Content-Length: 0

6.5.2.4. Call termination to disconnection (IPv4, Use of timer and 100rel, G.711 μ-law)

This clause shows a message flow on the terminating side under the same condition of option item selections as Annex Table p-1. After receiving a call from the network, session refresh is performed by *UPDATE*, and disconnection (by the terminating side) is performed by *BYE*. The network notifies the calling-party's identity information by the *P-Asserted-Identity* header, and the called-party's information by the *P-Called-Party-ID* header to the called terminal.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10
IP (RTP): 192.0.1.11

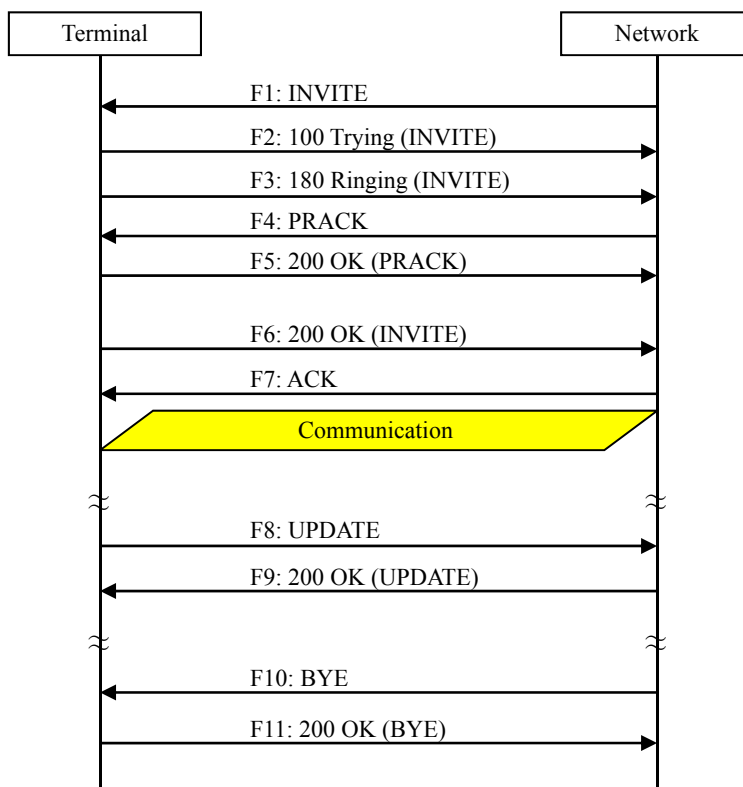


**Figure 8 Call termination to disconnection
(IPv4, Use of timer and 100rel, G.711 μ-law)**

▪ **F1: INVITE**

INVITE sip:qwertyui@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>
From: <sip:0312222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10

```

CSeq: 101 INVITE
Contact: <sip:lkjhgfds@192.0.1.10>
P-Asserted-Identity: "032222223" <sip:032222223@example1.ne.jp>,"03222
2223" <tel:032222223;phone-context=example1.ne.jp>
Privacy: none
P-Called-Party-ID: <sip:031111112@example1.ne.jp>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82664482616 82664482616 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 40000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20

```

- **F2: 100 Trying**

```

SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
To: <sip:031111112@example1.ne.jp>
From: <sip:032222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Content-Length: 0

```

- **F3: 180 Ringing**

```

SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:031111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:032222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0

```

- **F4: PRACK**

```

PRACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
Max-Forwards: 64
To: <sip:031111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:032222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10

```

```
CSeq: 102 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

▪ **F5: 200 OK (PRACK)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
To: <sip:031111112@example1.ne.jp>;tag=1234abcd-1111121
From: <sip:032222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 102 PRACK
Content-Length: 0
```

▪ **F6: 200 OK (INVITE)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:031111112@example1.ne.jp>;tag=1234abcd-1111121
From: <sip:032222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 30000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

▪ **F7: ACK**

```
ACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101022
Max-Forwards: 70
To: <sip:031111112@example1.ne.jp>;tag=1234abcd-1111121
From: <sip:032222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 ACK
Content-Length: 0
```

- **F8: UPDATE**

```
UPDATE sip:lkjhgfds@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
Max-Forwards: 70
To: <sip:032222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:031111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

- **F9: 200 OK (UPDATE)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
To: <sip:032222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:031111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:lkjhgfds@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

- **F10: BYE**

```
BYE sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
Max-Forwards: 70
To: <sip:032222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:031111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

- **F11: 200 OK (BYE)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
To: <sip:032222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:031111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

6.5.2.5. Call cancellation (disconnection while ringing)

This clause shows an example message flow for call cancellation by the originating side under the same condition of option item selections as in Annex Table p-1.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10
IP (RTP): 192.0.1.11

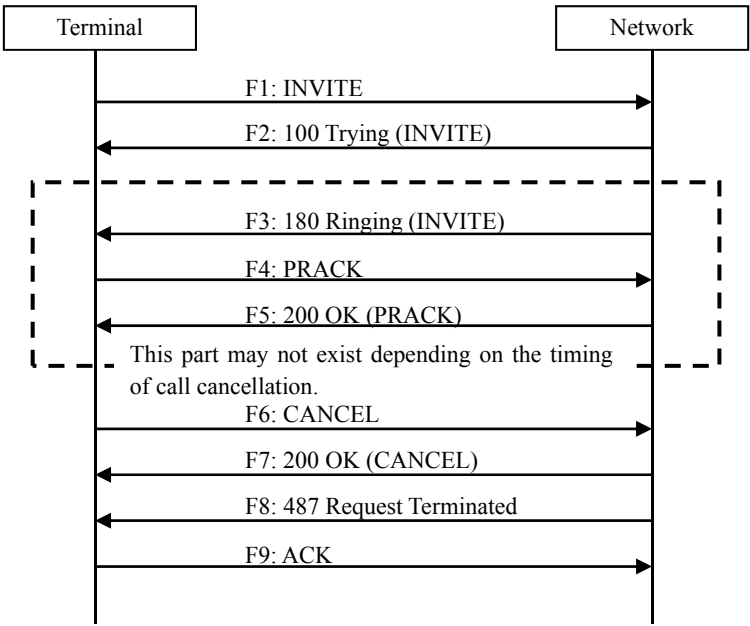


Figure 9 Call cancellation (disconnection while ringing)

F1 to F5 are omitted because they are the same as those of clause Annex Table p-1.

▪ **F6: CANCEL**

```
CANCEL tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

▪ **F7: 200 OK (CANCEL)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

- **F8: 487 Request Terminated**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

- **F9: ACK**

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

6.5.2.6. Busy on the terminating side

This clause shows a message flow in the case that the destination is busy (short of empty sessions) under the same condition of option item selections as Annex Table p-1.

SIP domain: example1.ne.jp

TEL: 03-1111-1111, 03-1111-1112

IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10

IP (RTP): 192.0.1.11

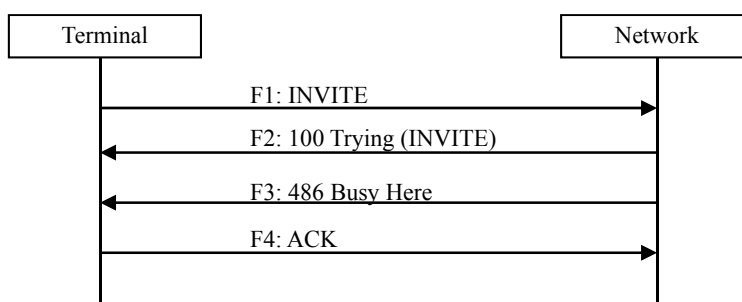


Figure 10 Busy on the terminating side

F1 to F2 are omitted because they are the same as those of clause Annex Table p-1.

F3: 486 Busy Here

```
SIP/2.0 486 Busy Here
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
```

```
CSeq: 1 INVITE
Content-Length: 0
```

F4: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

6.6. Test scenario of VoIP interoperability testing of the End-to-End service

This paragraph shows the detail steps for each test to prevent the omission of VoIP interoperability testing of the End-to-End service. This step should be tested after NIT confirmation in 6.5.

Figure 11 shows a sample of the general configuration of VoIP interoperability testing of the End-to-End service and follow this is the sample that shows test steps.

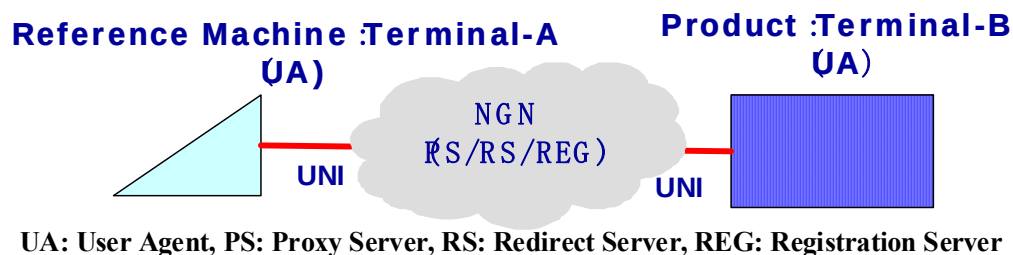


Figure 11 General Configuration of VoIP interoperability testing of the End-to-End service

6.6.1. Test items

Following is the sample of test items.

- A) Register a UA in the server.
- B) “Calling UA” calls “Receiving UA”. Checking PRACK request and OK response.
- C) If the call is not received, try calling again up to 3 times. If the call is still not received, check the communication conditions, such as the registration information. If something is wrong with the conditions, then retry from (A); otherwise, consider this as a communication error and conduct procedure (G).

- D) After confirming the connection, the receiving UA checks that it can properly receive the audio, video (if required), and other test items from the other terminal in accordance with the items listed. Also, the encoding mode that has executed the communication for the caller or the receiver must be recorded respectively for Calling UA or Receiving UA.
- E) Continue the communication for at least 3 minutes. Then, check if all the items have been tested. Check if the session timer is updated by UPDATE request and OK response.
- F) Both the caller and the receiver must confirm that the communication can be disconnected properly.
- G) Switch roles of the caller and the receiver, and repeat procedures (A) to (F).

Test criteria of each test items should be described to clarify the conformance test verifications. Table 3 is a sample of test criteria.

Table 3 Test criteria

Nº	Item		Judging standard
1	Sending side (Terminal A)	Terminal registration	Confirm the communication of audio and the video in each mode for more than 3 minuets.
2		Confirmation of Audio communications	
3		Transmission rate of Audio	Confirm PRACK request and OK response. Confirm the session timer is updated by UPDATE request and OK response at least one time.
4		Other	Record the maximum transmission rate capability that was exchanged.
5		Disconnection by Network	If required
6		Disconnection by terminal	Confirm that Terminal disconnected properly when Terminal disconnected.

Nº	Item		Judging standard
1	Receiving side (Terminal B)	Terminal registration	Confirm the communication of audio and the video in each mode more than 3 minuets.
2		Confirmation of Audio communications	
3		Transmission rate of Audio	Confirm PRACK request and OK response. Confirm a session timer is updated by UPDATE request and OK response at least one time.
4		Other	Record the maximum transmission rate capability that was exchanged.
5		Disconnection by Network	If required
		Disconnection by terminal	Confirm that Terminal disconnected properly when Terminal disconnected.

6		Disconnection by terminal	Confirm that Terminal disconnected properly when Terminal disconnected.
---	--	---------------------------	---

7. Analyze the test output

The test outcomes are assumed to be as follows: Such as a test event, an examination log, and a state, output as a test outcome in Test campaigns are compared, and the NGN service of the examination target device and the confirmation of adaptability

The test outcomes (such as the output test event, test logs and statement of the tested product) as service testing results in Test campaigns should be compared with the specification of the Recommendations.

7.1. Test report production

This paragraph shows the methods to make a summary of the examinations for the test result successes and failures and shows the detailed items required for success of the tests in order to illustrate the results of the conformance test.

Test result will show two items about NIT (Network Integration Test) for service test and VoIP interoperability testing of the End-to-End service.

Table 4 and 5 shows a sample Verification sheet.

Table 4 Verification sheet of NIT

Item		Result	
		Success	Failure
(a)	Terminal registration (access-line based authentication)		
(b)	Deletion of terminal registration (access-line based authentication)		
(c)	Call origination to disconnection (IPv4, Use of timer and 100rel, G.711 μ -law)		
(d)	Call termination to disconnection (IPv4, Use of timer and 100rel, G.711 μ -law)		
(e)	Call cancellation		
(f)	Busy on the terminating side		

Table5 VoIP interoperability testing of the End-to-End service

Item	Result
------	--------

			Success	Failure
1	Sending side (Terminal A)	Terminal registration		
2		Confirmation of Audio communications		
3		Transmission rate of Audio		
4		Other (if required)		
5		Disconnection by Network		
6		Disconnection by terminal		

	Item	Result	
		Success	Failure
1	Sending side (Terminal B)	Terminal registration	
2		Confirmation of Audio communications	
3		Transmission rate of Audio	
4		Other (if required)	
5		Disconnection by Network	
6		Disconnection by terminal	

ANNEX

Additional specifications to NGN UNI Signalling Profile (Protocol Set 1)

Contents

Annex a.	Clarification and option lists of Q3402 main body	31
a.1.	Overview	31
a.2.	References	31
a.3.	Clarification and option lists	31
Annex b.	Calling line identification presentation and related headers	37
b.1.	Overview	37
b.2.	References	37
b.3.	Network-asserted user identity	37
b.3.1.	Notification when the terminal registers	37
b.4.	Calling party numbers	37
b.4.1.	Procedures on originating a call	38
b.4.1.1.	Selecting a calling-party identity	38
b.4.1.2.	Setting for presentation/restriction of calling-party identity	38
b.4.2.	Procedures on receiving a call	39
b.4.2.1.	In the case that calling-party identity, cause of no ID, etc. are notified	39
b.4.2.2.	In the case that calling-party identity, cause of no ID, etc. are not notified	40
b.5.	Destination notification	40
b.6.	URI format in the case that a national number is used	40
b.6.1.	user part and local-number-digits part	41
b.6.2.	hostport part and descriptor part of context	41
b.7.	Subaddress	41
b.7.1.	Subaddress information	41
b.7.1.1.	Contents of subaddress information	41
b.7.1.2.	Formats of subaddress information	41
Annex c.	Registration	42
c.1.	Overview	42
c.2.	Obtaining the network address	42
c.3.	Registration	42
c.3.1.	path extension function and Service-Route header	42
c.3.2.	pre-existing route	42
c.3.3.	Difference of address format retained by network	42
c.4.	Refresh	43
c.5.	Deletion	43
c.5.1.	Considerations on terminal halt and IP address modification	43
c.6.	Registration event	43
c.6.1.	Subscription to registration event	43
c.6.2.	Notification of registration event	43
Annex d.	SIP capabilities exchange	44

d.1.	Overview	44
d.2.	Available methods.....	44
d.2.1.	UPDATE.....	44
d.2.2.	PRACK.....	44
d.3.	Extension function	44
d.3.1.	Session timer function (timer)	44
d.3.2.	Provisional response reliability function (100rel).....	44
Annex e.	SDP and media handling.....	45
e.1.	Overview	45
e.2.	Judging a media change request	45
e.2.1.	Receiving SDP.....	45
e.2.2.	Sending SDP.....	45
e.3.	Payload type	45
e.4.	Fallback procedure.....	45
e.4.1.	IP version incompatibility	45
e.4.2.	Media type incompatibility	46
Annex f.	Congestion prevention and control	47
f.1.	Overview	47
f.2.	Considerations on congestion control at time of registration	47
f.2.1.	Actions on receiving an error response.....	47
f.2.2.	Actions on receiving no response	47
f.2.3.	Considerations on registering multiple Contact addresses.....	47
f.2.4.	User name or password error	47
f.2.5.	Re-registration at the occurrence of temporary faults	47
f.3.	Considerations on congestion control when originating a call.....	48
f.3.1.	Congestion notification.....	48
f.3.1.1.	Notification to a terminal from a network.....	48
f.3.1.2.	Notification from a terminal to a user	48
f.3.2.	Additional information notification	48
f.3.2.1.	Notification from a network to a terminal.....	48
f.3.2.2.	Notification from a terminal to a user	49
f.3.3.	User name or password error	49
Annex g.	Bandwidth control	50
g.1.	Overview	50
g.2.	References	50
g.3.	Bandwidth control mechanism in NGN.....	50
g.3.1.	Resource and Admission Control Functions.....	51
g.3.2.	Policing function.....	52
g.3.2.1.	Behaviour of policer	52
g.3.2.2.	Token supplying rate.....	54
g.4.	SIP/SDP specifications	54
g.4.1.	Specifying RTP bandwidth	54

g.4.1.1.	Considerations on overhead in lower layers.....	54
g.4.1.2.	Considerations on burstiness.....	54
g.4.2.	RTCP bandwidth.....	55
g.5.	Quality class	55
g.5.1.	Multiple quality classes and DiffServ	55
g.5.2.	Setting of DSCP value	56
Annex h.	Constraints on string length and value range of SIP messages	57
h.1.	Overview	57
h.2.	String length and value range	57
h.2.1.	SIP	57
h.2.2.	SDP.....	58
Annex i.	Audio terminal behaviour	59
i.1.	Overview	59
i.2.	Codec.....	59
i.2.1.	Packetization period.....	59
i.3.	Behaviour at time of disconnection	59
i.3.1.	Sending a CANCEL/BYE request	59
i.3.2.	Receiving a CANCEL/BYE request (before final response)	59
i.3.3.	Receiving a CANCEL request (after final response)	60
i.3.4.	Receiving a 3xx response	60
i.3.5.	Receiving a 4xx to 6xx response.....	60
i.3.6.	Sending a 4xx to 6xx response.....	60
i.4.	Ringtone generation and dialog management.....	60
i.4.1.	Sending a 18x response.....	60
i.4.2.	Receiving a 18x response	60
i.4.2.1.	Ringtone generation	60
i.4.2.2.	Early media generation	61
i.4.3.	Receiving a 2xx response	61
i.4.3.1.	Management of multiple dialogs and media	61
i.5.	Media change.....	62
i.5.1.	IP address and port number.....	62
Annex j.	Option items	63
j.1.	Introduction	63
j.2.	Option item extraction policy	63
j.3.	Option item table format.....	63
j.4.	Option item table	63
Annex k.	Response code usage	80
k.1.	Introduction	80
k.2.	4xx response	80
k.2.1.	403 Forbidden.....	80
k.2.2.	404 Not Found	80
k.2.3.	410 Gone	80

k.2.4.	433 Anonymity Disallowed	81
k.2.5.	480 Temporarily Unavailable.....	81
k.2.6.	486 Busy Here	81
k.2.7.	487 Request Terminated	81
k.2.8.	488 Not Acceptable Here	81
k.3.	5xx response	81
k.3.1.	503 Service Unavailable	81
Annex l.	Mapping SDP description to QoS classes	83
l.1.	Overview	83
l.2.	Concept.....	83
l.3.	Example of correspondence	83
l.3.1.	SDP	83
Annex m.	Security considerations	85
m.1.	Overview	85
m.2.	Requirements for the UNI.....	85
m.3.	Solution examples.....	85
m.3.1.	Filtering with source IP address	85
m.3.2.	Limiting the port for use	85
m.3.3.	Randomization of a Contact header (on terminal registration)	86
m.3.4.	Randomization of a Contact header (on initiating sessions)	86
m.3.5.	Considerations on transparent transfer of SIP messages	86
Annex n.	Discovery procedure of the SCF	87
n.1.	Overview	87
n.2.	References	87
n.3.	DHCP/DHCPv6	87
n.4.	Terminal preconfiguration	87
Annex o.	Signalling rule of SIP messages and headers	88
o.1.	Dynamic view and static view	88
o.1.1.	Static view	88
o.1.2.	Dynamic view	88
o.1.3.	Adoption of dynamic view for this annex.....	88
o.1.4.	Definition of notation codes in the tables in this annex	88
o.2.	ACK.....	90
o.2.1.	Supported headers in the ACK request	90
o.2.2.	Supported headers in the ACK response	91
o.3.	BYE	92
o.3.1.	Supported headers in the BYE request	92
o.3.2.	Supported headers in the BYE response	94
o.4.	CANCEL	96
o.4.1.	Supported headers in the CANCEL request	96
o.4.2.	Supported headers in the CANCEL response	97
o.5.	INVITE.....	98

o.5.1.	Supported headers in the INVITE request	98
o.5.2.	Supported headers in the INVITE response	101
o.6.	MESSAGE	104
o.6.1.	Supported headers in the MESSAGE request	104
o.6.2.	Supported headers in the MESSAGE response	106
o.7.	NOTIFY	108
o.7.1.	Supported headers in the NOTIFY request	108
o.7.2.	Supported headers in the NOTIFY response	110
o.8.	PRACK	112
o.8.1.	Supported headers in the PRACK request	112
o.8.2.	Supported headers in the PRACK response	114
o.9.	PUBLISH	116
o.9.1.	Supported headers in the PUBLISH request	116
o.9.2.	Supported headers in the PUBLISH response	118
o.10.	REFER	120
o.10.1.	Supported headers in the REFER request	120
o.10.2.	Supported headers in the REFER response	122
o.11.	REGISTER	124
o.11.1.	Supported headers in the REGISTER request	124
o.11.2.	Supported headers in the REGISTER response	126
o.12.	SUBSCRIBE	128
o.12.1.	Supported headers in the SUBSCRIBE request	128
o.12.2.	Supported headers in the SUBSCRIBE response	130
o.13.	UPDATE	132
o.13.1.	Supported headers in the UPDATE request	132
o.13.2.	Supported headers in the UPDATE response	134
Annex p.	Message examples	136
p.1.	Sequence examples	137
p.1.1.	Terminal registration (access-line based authentication)	137
p.1.2.	Terminal registration (HTTP Digest authentication)	139
p.1.3.	Deletion of terminal registration (access-line based authentication)	141
p.1.4.	Call origination to disconnection (IPv4, Use of timer and 100rel, G.711 μ -law)	143
p.1.5.	Call origination to disconnection (IPv4, Use of timer and 100rel, G.711 μ -law, HTTP Digest authentication)	147
p.1.6.	Call termination to disconnection (IPv4, Use of timer and 100rel, G.711 μ -law)	150
p.1.7.	Call cancellation (disconnection while ringing)	154
p.1.8.	Busy on the terminating side	156
p.1.9.	Hearing the guidance	157
p.1.10.	Connection after hearing the guidance (using UPDATE)	159
p.1.11.	Sending MESSAGE (using IPv6)	161
p.1.12.	Receiving MESSAGE (using IPv6)	162
p.1.13.	Subscription to registration event	163
p.1.14.	Notification of registration event (on deletion of terminal registration)	165

This Annex provides additional specifications to ITU-T Recommendation Q.3402 in order to define more detailed protocol specifications.

- (a) Clarifications on the specifications, network options, and terminal options of the Q3402 main body in order to improve the interoperability of SIP terminals connected to domestic NGN carriers through the UNI.
This annex shows the clarifications in tables with the corresponding clause number of the main body; follow the content of this annex in addition to the main body. (Annex a)
- (b) Calling line identification presentation (Annex b)
- (c) Terminal registration (Annex c)
- (d) Negotiating SIP capabilities (Annex d)
- (e) SDP setting and media handling (Annex e)
- (f) Considerations on congestion prevention and control (Annex f)
- (g) Bandwidth control (Annex g)
- (h) Limitations of SIP message settings (Annex h)
- (i) Audio terminal's behaviour (Annex i)
- (j) List of network options and terminal options for this standard (Annex j)
- (k) Guidelines for response code usage (Annex k)
- (l) Mapping SDP description to QoS classes (Annex l)
- (m) Security considerations (Annex m)
- (n) Discovery procedure of the SCF (Annex n)
- (o) Signalling rule tables of SIP messages and headers (Annex o)
- (p) Examples of message flows (Annex p)

Annex a. Clarification and option lists of Q3402 main body

(This annex is a normative part of this standard.)

a.1. Overview

This annex provides clarification and option lists of the Q3402 main body to improve the interoperability of SIP terminals to the NGN connected through the UNI in the architecture defined in the Q3402 main body.

a.2. References

References used in this annex are as follows.

- [RFC4585] "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)", TTC standard JF-IETF-RFC4585, version 1.0, March 2008
- [RFC5104] "Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)", TTC standard JF-IETF-RFC5104, version 1.0, March 2008
- [RFC5407] "Example calls flows of race conditions in the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC5407, version 1.0, May 2009

a.3. Clarification and option lists

Annex Table a-1 shows the clarification and option lists for the main body of Q3402. Clauses unmentioned in the table mean that specifications in the base document are applied as they are. Lists of options described in Annex a to Annex i and Annex j to Annex o are not shown in Annex Table a-1. Refer to Annex j for lists of options including these annexes and appendices.

Annex Table a-1/ JT-Q3402: Clarification and option lists

Clause of Q3402 main body		Clarifications	Options	Remarks
No.	Name of clause			
2.	References	References needed for this standard are described in each annex in addition to the base document.	—	
5	Reference model	In the case that the EUF is an audio telephone terminal, follow Annex i.	—	
6.	Assumptions	2. SRTP is not to be used for the transfer of audio and video	—	
7.1	Consideration related to media packets	Specifications in the base document are applied as they are.	Sending media packets from the originating terminal, in the case that a <i>1xx</i> response to <i>INVITE</i> includes SDP answer. (Annex Table j -25, Item 1) Handling of media packets before completion of SDP negotiation to an initial <i>INVITE</i> (Annex Table j -25, Item 2)	
8.1	Codec list	The audio codec list shall contain G.711 μ -law. Even when a codec in the codec list is set in an SDP offer, it may not be end-to-end negotiation, depending on a carrier's policy. A codec that is not contained in the codec list is not to be set in an SDP offer.	Codecs to be contained in the codec list other than G.711 μ -law. (Annex Table j -16, Items 1 to 3)	
8.2	Packetization size	For the packetization period in the case of using G.711 μ -law, follow	—	

		Annex i.2.1.		
9.	Routing and addressing	For the URI format in the case of using a national number, follow Annex b.6. For the subaddress, follow Annex b.7.	<i>Request-URI</i> format of SIP requests outside existing dialogs, except for <i>REGISTER</i> . (Annex Table j -20, Items 1 and 2)	
10.1	RFCs to be supported	RFC2976, RFC3388, RFC3725, RFC3824, RFC3853, RFC3861, RFC3959, RFC3960, RFC4168, RFC4244, RFC4412, RFC4458, and RFC5031 are not to be used. Support for the <i>P-Media-Authorization</i> header specified in RFC3313 is applicable only in the direction from the SCF to the EUF. For the handling of the <i>Reason</i> header specified in RFC 3326, follow Annex f.3.1. For the handling of the path extension function specified in RFC 3327, follow Annex c.3. Support for the <i>Path</i> header is applicable only to the response in the direction from the SCF to the EUF. Support for the <i>Security-Client</i> header and <i>Security-Verify</i> header specified in RFC3329 is applicable only to the request in the direction from the EUF to the SCF, and support for the <i>Security-Server</i> header is applicable only to the response in the direction from the SCF to the EUF. Of the headers specified in RFC3455, the <i>P-Associated-URI</i> header and the <i>P-Called-Party-ID</i> header are used, which conform to Annex b. The headers <i>P-Charging-Vector</i>, <i>P-Charging-Function-Addresses</i>, and <i>P-Visited-Network-ID</i> are not to be used. Support for the <i>P-Access-Network-Info</i> header is applicable only to the SIP messages in the direction from the EUF to the SCF. For the handling of the <i>Service-Route</i> header specified in RFC 3608, follow Annex c.3. For the registration event specified in RFC 3680, follow Annex c.6.	The followings are the list of options for each RFC. [RFC2046] Use of MIME Multipart (Annex Table j -10, Items 1 to 4) [RFC3310, RFC2617, and RFC3329] Terminal authentication procedures (Annex Table j -11, Items 1 and 2) Use of security capabilities exchange function (<i>sec-agree</i>) (Annex Table j -7, Item 8) [RFC3262] Use of provisional response reliability function (<i>100rel</i>) (Annex Table j -7, Item 2) [RFC3265] Use of <i>SUBSCRIBE</i> method and <i>NOTIFY</i> method. (Annex Table j -2, Items 10 to 15) [RFC3311] SDP offer by <i>UPDATE</i> (Annex Table j -23, Items 1, 2, 5, and 6) Media modification in early dialog (Annex Table j -23, Items 1 and 2) [RFC3312, RFC4032] Use of function for reserving bandwidth before session establishment (<i>precondition</i>) (Annex Table j -7, Item 5) [RFC3313] Use of <i>P-Media-Authorization</i> header (Annex Table j -17, Item 1) [RFC3320, RFC3485, RFC3486, RFC5049] Use of SigComp (Annex Table	

		Note: To support RFCs means to follow the contents described in the RFCs. It does not mean that their capabilities are used in all sessions.	j -5, Item 1) [RFC3388, RFC3524] Use of Grouping of media (Annex Table j -18, Item 1) [RFC3428] Use of <i>MESSAGE</i> method (Annex Table j -2, Items 2 to 5) [RFC3515, RFC3892] Use of <i>REFER</i> method (Annex Table j -2, Items 6 to 9) [RFC3556] Use of SDP bandwidth modifier for RTCP bandwidth (Annex Table j -13, Item 4) [RFC3581] Allowing Hosted NAT in the lower part of UNI (Annex Table j -6, Item 1) [RFC3840, RFC3841] Use of terminal capabilities notification function (<i>pref</i>) (Annex Table j -7, Item 6) [RFC3891] Use of dialog replacement function (<i>replaces</i>) (Annex Table j -7, Item 3) [RFC3903] Use of <i>PUBLISH</i> method (Annex Table j -2, Items 16 to 19) [RFC3911] Use of conference session participation function (<i>join</i>) (Annex Table j -7, Item 4) [RFC4028] Session refresh by <i>UPDATE</i> method (Annex Table j -8, Item 1)	
10.2.1.7	SIP Messages	For maximum length of SIP messages and its elements, follow Annex h.	–	
10.2.1.7.1	Requests	<i>OPTIONS</i> method is not to be used. SIPS-URI is not to be used.	–	
10.2.1.7.4.1	Message body types	Specifications in the base document are applied as they are.	SDP settings for <i>PRACK</i> and <i>200 OK</i> to <i>PRACK</i> . (Annex Table j -22, Items 2 and 3)	
10.2.1.8.1.3	Processing responses	Specifications in the base document are applied as they are.	Terminal authentication procedures (Annex Table j -	

			11, Items 1 and 2)	
10.2.1.8.3	Redirect servers	Specifications in the base document are applied as they are. The 3xx response is applicable to requests outside existing dialogs, except for <i>REGISTER</i> .	Use of redirect functions by 3xx response (Annex Table j -12, Items 1 and 2)	
10.2.1.10	Registrations	For the terminal registration procedures, follow Annex c. For the congestion control at the time of terminal registration, follow Annex f.2.	Whether or not terminal registration needed and procedures (Annex Table j -2, Item 1, Annex Table j -11, Item 1, and Annex Table j -24, Items 1 to 5)	
10.2.1.11	Querying for capabilities	Querying for capabilities is not supported.	–	
10.2.1.12.1	Creation of a dialog	SIPS-URI is not to be used.	–	
10.2.1.12.2	Requests within a dialog	SIPS-URI is not to be used.	–	
10.2.1.13	Initiating a session	Initial <i>INVITE</i> includes an SDP offer which contains valid media. (SDP negotiation using 2xx/ <i>ACK</i> is not to be used.) Follow Annex f.3 for congestion control at the time of call origination.	–	
10.2.1.14	Modifying an existing session	In the case of using re- <i>INVITE</i> , SDP offer is set in <i>INVITE</i> request.	Media modification after a dialog is established. (Annex Table j -23, Items 3 to 6)	
10.2.1.17	Transactions	For the processing at race conditions triggered by SIP signalling crossover etc., conform to [RFC5407]. Note that this standard lists a sequence between SIP-UAs, and when applying to the UNI, it should be read as sequence between network and terminal.	–	
10.2.1.19	Common message components	SIPS-URI is not to be used.	–	
10.2.1.20.7	Authorization	The Authorization header is used only when the SCF authenticates a <i>REGISTER</i> request from the EUF.	–	
10.2.1.20.11	Content-Disposition	Only the default value can be set in the parameter of the <i>Content-Disposition</i> header. Application server model as defined in RFC3959 is not to be used.	–	
10.2.1.20.27	Proxy-Authenticate	The <i>Proxy-Authenticate</i> header is used only in the 407 response when the SCF authenticates a request sent from the EUF outside existing dialogs except for <i>REGISTER</i> .	–	
10.2.1.20.28	Proxy-Authorization	The <i>Proxy-Authorization</i> header is used only when the SCF authenticates a request sent from the EUF outside existing dialogs except for <i>REGISTER</i> .	–	
10.2.1.20.29	Proxy-Require	The <i>Proxy-Require</i> header is applicable only in the direction from	–	

		the EUF to the SCF.		
10.2.1.20.24	MIME-Version	Only "1.0" is supported	–	
10.2.1.20.32	Require	Application server model as defined in RFC3959 is not to be used.	Use of <i>timer</i> , <i>100rel</i> , and other SIP option tags (Annex Table j -7, Items 1 to 9)	
10.2.1.20.33	Retry-After	For congestion control, the <i>Retry-After</i> header is utilized as described in Annex f.2.1.	–	
10.2.1.20.34	Route	For the pre-existing route, follow Annex c.3.	–	
10.2.1.20.44	WWW-Authenticate	The <i>WWW-Authenticate</i> header is used only in <i>401</i> responses when the SCF authenticates a <i>REGISTER</i> request from the EUF.	–	
10.2.1.23	S/MIME	S/MIME is not to be used for SDP with SIP messages related to <i>INVITE</i> .	–	
10.2.2.1	Extension method	For <i>UPDATE</i> and <i>PRACK</i> requests, follow Annex d.	–	
10.2.2.2.2	P-Asserted-Identity	The <i>P-Asserted-Identity</i> header is used only in requests outside existing dialogs except for <i>REGISTER</i> . For calling line identification presentation, follow Annex b.	–	
10.2.2.2.3	P-Preferred-Identity	The <i>P-Preferred-Identity</i> header is used only in requests outside existing dialogs except for <i>REGISTER</i> . For calling line identification presentation, follow Annex b.	–	
10.2.2.2.4	Privacy	The <i>Privacy</i> header is used only in requests outside existing dialogs except for <i>REGISTER</i> . Only " <i>id</i> " and " <i>none</i> " can be used for privacy options. For calling line identification presentation, follow Annex b.	–	
10.2.3	Summary of SIP methods and headers	<i>OPTIONS</i> method is not to be used.	SIP methods to be used (Annex Table j -2, Items 1 to 21)	
10.3.1	SDP usage	For the handling of SDP, follow Annex e. For the values specified in <i>b=</i> line, follow Annex g.	SDP lines to be used (Annex Table j -22, Items 4 and 5) IP version to be used for media (Annex Table j -3, Item 3) Use of video (<i>m=video</i>) and data communication (<i>m=application</i> , <i>m=data</i> , etc.) (Annex Table j -14, Items 1 and 2) Use of TCP for media [RFC 4145] (Annex Table j -14, Item 3)	
11.1	Specifications to be supported	Specifications in the base document are applied as they are. Feedback function utilizing RTCP	Use of feedback function utilizing RTCP (Annex Table j -19, Items 1 and 2)	

		(RTP/AVPF)[RFC4585][RFC5104] can be used.		
12	Call control signalling transport	UDP or TCP is used as transport protocol for sending and receiving SIP messages. TLS may be used for security.	Layer 4 protocol for call control signals (Annex Table j -4, Items 1 to 3)	
13	IP protocol version	Specifications in the base document are applied as they are. Refer to Annex e.4.1 for a note of IPv4/IPv6 fallback.	Layer 3 protocol for call control signals (Annex Table j -3, Items 1 to 4)	

.....

Annex b. Calling line identification presentation and related headers

(This annex is a normative part of this standard.)

b.1. Overview

This annex clarifies procedures for calling line identification presentation and notification of "cause of no ID", SIP headers used for them (*P-Preferred-Identity*, *P-Asserted-Identity*, *Privacy*, and *From*) and *Request-URI*, the SIP header used for relevant network-asserted user identity (*P-Associated-URI*), and the SIP header used for called party notification (*P-Called-Party-ID*).

b.2. References

References used in this annex are as follows.

[TS-1008] "Technical Specification on ISDN Called Party Subaddress Information Transferring through Provider's SIP Networks", TTC standard TS-1008, version 1, The Telecommunication Technology Committee, June 2004

b.3. Network-asserted user identity

The network-asserted user identity is the identity of a user that is asserted by the network through authentication or other means (verified by the network if provided by the terminal), and it is used for calling-party identity, etc. An example of network-asserted user identity information is a SIP-URI composed of an E.164 number reachable to the terminal. As described in clause b.7, subaddress information may be provided by the calling terminal.

Clause b.6 indicates a specific URI format for network-asserted user identity.

b.3.1. Notification when the terminal registers

In the case of using a *REGISTER* request for registration, the network may set a *P-Associated-URI* header [RFC3455] in its *200 OK* response in order to notify a network-asserted user identity to the terminal. [Annex Table j -24, Item 3]

A *P-Associated-URI* header lists one or more URIs which indicate network-asserted user identities allocated to the terminal. In the case that multiple network-asserted user identities are listed, the terminal recognizes the first URI as the default network-asserted user identity.

b.4. Calling party numbers

Calling party number (hereinafter referred to as calling-party identity) presentation should be realized based on JF-IETF-RFC3323[RFC3323], JF-IETF-RFC3324[RFC3324], and JF-IETF-RFC3325[RFC3325] by notifying network-asserted user identity and presentation/restriction information. Calling-party identity presentation/restriction are applied to requests outside existing dialogs except for *REGISTER* which can be sent and received over the UNI.

Calling-party identity information presentation is mainly performed by four steps as follows.

- 1) A calling terminal transmits the selected calling-party identity information (*P-Preferred-Identity*) and preference of presentation/restriction (*Privacy*) to a network, instructs a destination (*Request-URI*), and calls.
- 2) The network which has the calling party verifies and normalizes a calling-party identity that a terminal selected, takes into consideration the default presentation/restriction setting etc. regarding the subscriber, and determines a calling-party identity information transmitted in the network and through the NNI.
- 3) The network which has the called party takes into consideration the preference of presentation/restriction and the called party's subscription for calling-party identity presentation service, and determines a calling-party identity information to be notified to the called terminal.
- 4) The called terminal is notified of calling-party identity information from the network when receiving a call.

In this annex, clause b.4.1 describes step 1 and 2 as procedures on originating a call, and clause b.4.2 describes step 3 and 4 as procedures on terminating a call.

b.4.1. Procedures on originating a call

b.4.1.1. Selecting a calling-party identity

In the case that a terminal desires to explicitly select a calling-party identity among the network-asserted identities, the terminal populates the selected network-asserted user identity in *P-Preferred-Identity* header in requests outside existing dialogs. If network-asserted user identities are notified as described in clause b.3.1, the terminal selects one of the URIs listed in a *P-Associated-URI* header and populates it in the *P-Preferred-Identity* header.

The network handles a SIP-URI set in the *P-Preferred-Identity* header as calling-party identity. Note that in the case the *P-Preferred-Identity* header is not set, or a URI set in the *P-Preferred-Identity* header is not a network-asserted user identity allocated to the calling terminal, it is to be the same as when the default network-asserted user identity is set in the *P-Preferred-Identity* header.

b.4.1.2. Setting for presentation/restriction of calling-party identity

When a terminal sends requests outside existing dialogs, calling-party identity presentation/restriction is requested using two kinds of procedures, namely, *Privacy* header [RFC3325] and 186/184 prefixes.

- Calling-party identity presentation can be requested by setting "none" in *Privacy* header, and restricted by setting "id". The *Privacy* header is set only when the terminal has the user configuration option of calling-party identity presentation/restriction, and the user completes the setting.
- In the case that the *Request-URI* is a URI composed of a national telephone number, calling-party identity presentation is specified when the 186 prefix is set, and restriction is specified when the 184 prefix is set. Whether to set the 186/184 prefix must be left to the decision of a dialling user, and a terminal must not act on its own, such as automatically putting the prefix.

The settings of the *Privacy* header and those of the 186/184 prefix are independent of each other.

In the case that the terminal sets "id" in a *Privacy* header, <sip:anonymous@anonymous.invalid> is set to the SIP-URI of a *From* header. In other cases, a URI identical to that of a *P-Preferred-Identity* header is set.

Annex Table b-1 describes the contents set in the headers above.

Annex Table b-1/JT-Q3402: Settings of headers for calling line identification presentation

Field	Privacy header		
	none	id	No header
The user part or telephone-subscriber part of a <i>Request-URI</i>	Number that a user dialled (includes 186/184 prefix if dialled)		
<i>P-Preferred-Identity</i> header	Calling-party's network-asserted user identity		
URI in <i>To</i> header	Same value as <i>Request-URI</i>		
<i>name-addr</i> in <i>From</i> header	Same value as the URI set in a <i>P-Preferred-Identity</i> header, if the header is set	<sip:anonymous@anonymous.invalid>	Same value as the URI set in a <i>P-Preferred-Identity</i> header, if the header is set

A network selects calling-party identity presentation/restriction, based on the *Privacy* header and 186/184 prefix setting, and the default calling-party identity presentation/restriction setting of a subscriber who originates a call.

- In the case that a 186/184 prefix is set at the beginning of the telephone number in the *Request-URI*, the call is treated to be calling-party identity presentation when 186 is set, and calling-party identity restriction when 184

is set, regardless of a *Privacy* header setting content.

- The default calling-party identity presentation setting of the subscriber who originates the call is applied when neither the *Privacy* header setting nor a 186/184 prefix setting exists.
- In the case that the 184 prefix is not set, it is treated to be calling-party identity presentation, regardless of a *Privacy* header setting content, at the time of emergency call.

Annex tables b-2 and b-3 describe the order of priority among the *Privacy* header settings, 186/184 prefix settings, and the default calling-party identity presentation/restriction setting above.

Annex Table b-2/JT-Q3402: Calling-party identity presentation/restriction selection conditions for normal call

		Prefix of destination number		
		186	184	No prefix
<i>Privacy</i>	<i>none</i>	Calling-party identity presentation	Calling-party identity restriction	Calling-party identity presentation
	<i>id</i>			Calling-party identity restriction
	No header			Follow the default value of the network managed for each calling user

Annex Table b-3/JT-Q3402: Network selected conditions of presentation/restriction of calling-party identity for emergency call

		Prefix of a destination number		
		186	184	No prefix
<i>Privacy</i>	<i>none</i>	Calling-party identity presentation	Calling-party identity restriction	Calling-party identity presentation
	<i>id</i>			
	No header			

In the case that the calling-party identity is restricted, "*Anonymous*" (No caller ID: rejected by user) is selected as cause of no ID out of causes described in Annex Table b-4.

b.4.2. Procedures on receiving a call

The SIP headers on the terminating side are populated according to the called-party's subscription of calling-party identity presentation/restriction.

b.4.2.1. In the case that calling-party identity, cause of no ID, etc. are notified

The calling-party identity and cause of no ID, etc. are notified by setting a *Privacy* header in requests outside existing dialogs received from a network.

In the case that "*none*" is set in the *Privacy* header, calling-party identity is notified by a *P-Asserted-Identity* header. In the *P-Asserted-Identity* header, only a SIP-URI is set or both a SIP-URI and a TEL-URI are set.

In the case that "*id*" is set in the *Privacy* header, calling-party identity is not notified by the *P-Asserted-Identity* header. Instead, cause of no ID is set in *display-name* in a *From* header. In the case that calling-party identity is not notified, a displayed content (meaning) may be provided as cause of no ID in the form indicated in Annex Table b-4. Note that the cause of no ID is not provided in the case that a format is not as shown in Annex Table b-4.

Annex Table b-4/JT-Q3402: Cause of no ID

Received content ^(*) (*)	Display content (meaning)
<i>Anonymous</i>	No caller ID: rejected by user
<i>Coin line/payphone</i>	No caller ID: call from public telephone
<i>Interaction with other service</i>	No caller ID: service conflict
<i>Unavailable</i>	No caller ID: service unavailable

(*) It may be enclosed with a pair of double quotation marks.

(*) A character string listed in this table may be followed by a given character string.

b.4.2.1.1. Displaying calling-party identity

A terminal displays calling-party identity notified by a *P-Asserted-Identity* header according to the order of priority described below.

- 1) In the case that both a SIP-URI and a TEL-URI are set in a *P-Asserted-Identity* header, the TEL-URI is preferred for display.
- 2) In the case that *display-name* is set in the URI of a *P-Asserted-Identity* header, *display-name* is preferred for display rather than *addr-spec*.

In the case that *display-name* is not set, *user* part of a SIP-URI, *local-number-digits* part or *global-number-digits* part of a TEL-URI is displayed, and this part is a character string indicated in the display content in Annex Table b-5, a display content (meaning) corresponding to each case is indicated.

Annex Table b-5/JT-Q3402: Content of caller number display

Received content ^(*)	Display content (meaning)
Only numbers	Received numeric string
Starting with +81, and the part after + is composed of only numbers	Numeric string that omits +81 and starts with 0
Starting with +, the part after + is all composed of numbers, and the part next to + is not 81.	Numeric string that omits + and starts with 010

(*) When used as *display-name*, it may be enclosed with a pair of double quotation marks.

b.4.2.2. In the case that calling-party identity, cause of no ID, etc. are not notified

A *Privacy* header and a *P-Asserted-Identity* header are not set, and a character string which indicates cause of no ID is not set in *display-name* in a *From* header.

b.5. Destination notification

A network may populate a *P-Called-Party-ID* header [RFC3455] in requests outside existing dialogs to a called terminal, and may set a URI which indicates a network-asserted user identity of the destination.

In the case that multiple network-asserted user identities are allocated, a terminal uses a *P-Called-Party-ID* header in order to identify towards which network-asserted user identity a call is directed. In the case that the *P-Called-Party-ID* header is not set, it should be recognized that the call is directed to the default network-asserted user identity.

b.6. URI format in the case that a national number is used

This clause describes a URI format for the case using a national number as network-asserted user identity and *Request-URI*. Other URI formats may be used. [Annex Table j -20, Item 1]

A SIP-URI or a TEL-URI is used for network-asserted user identity. Either one or multiple SIP-URIs are allocated as network-asserted user identity for each user. A SIP-URI or a TEL-URI is used for *Request-URI*.

A subaddress described in clause b.7 may be set.

b.6.1. user part and local-number-digits part

In a SIP-URI, a numeric string of national number is described in *user* part, and in a TEL-URI, a numeric string of national number is described in *local-number-digits* part. Note that letters equivalent to *visual-separator* are not to be used in either *user* part or *local-number-digits* part.

In the case of *Request-URI*, a numeric string that a user dialled is set as it is in the *user* part or in the *local-number-digits* part. In the case of network-asserted user identity, all digits of a telephone number starting with a national prefix (i.e., "0") are set.

b.6.2. hostport part and descriptor part of context

The *hostport* part of a SIP-URI and the *descriptor* part of TEL-URI *context* are to be set as domain name or host name (including IP address) that a network specifies. [Annex 1-20, Item 2]

b.7. Subaddress

A network may provide services that are equivalent to services realized by the transfer of subaddress information that can be provided in the ISUP network through the interconnection interface as defined in JJ-90.10. [Annex Table j -9, Items 1 and 2]

This annex shows the usage of subaddress information in SIP messages based on [TS-1008] and complement the standard. The network and terminals, which handle subaddress information, are required to follow this clause and its subclauses. As for [TS-1008], follow the specifications for Interface B in [TS-1008]. In referring to the specifications of [TS-1008], "called party subaddress" should be read as "calling and called subaddress", and "providers' SIP network" as "network".

b.7.1. Subaddress information

b.7.1.1. Contents of subaddress information

The subaddress is a numeric string of 19 digits or less using numbers 0 to 9. The details are based on [RFC4715] and [TS-1008].

b.7.1.2. Formats of subaddress information

Subaddress information is applied to all the requests and responses of SIP messages and may be set in the headers that show the originating party (*From*, *P-Preferred-Identity*, *P-Asserted-Identity*), headers that show the terminating party (*To*, *P-Called-Party-ID*), and *Request-URI*. Subaddress is expressed as a numeric string following a semicolon (;) and "isub=" in the *user* part of SIP URI or TEL URI.

Annex c. Registration

(This annex is a normative part of this standard.)

c.1. Overview

This annex describes the procedures of terminal registration.

c.2. Obtaining the network address

A network provides a terminal with a means of notifying a SCF IP address and port number. The network provides DHCP/DHCPv6, presetting, and other procedures that depend on access line. [Annex Table j -24, Item 2]

The terminal transmits SIP messages to the obtained IP address and port number.

c.3. Registration

A terminal registers by sending to a network a *REGISTER* request in which a *Contact address* that it wants to register is set. A network may determine the setting conditions of the *q* parameter to the *Contact address*. [Annex Table j -24, Item 6]

The network may specify the *expires* parameter of a *Contact address* or the value set to an *Expires* header in the *REGISTER* request as a network option. [Annex Table j -24, Item 4]

c.3.1. path extension function and Service-Route header

A network may provide a pre-existing route using path extension function and *Service-Route* header. [Annex Table j -7, Item 7, Annex Table j -23, Item 1]

In the case that a network provides a pre-existing route, a terminal lists path extension function in *Supported* header as described in JF-IETF-RFC3327[RFC3327] and sends a *REGISTER* request. In the case that registration succeeds, a network sets a *Service-Route* header [RFC3608] in a *200 OK* response, and notifies the SIP-URI on or after the second hop of the pre-existing route.

c.3.2. pre-existing route

In the case that a pre-existing route is provided using procedures described in clause c.3.1, a terminal set the pre-existing route in *Route* header when sending requests outside existing dialogs except for *REGISTER*. The first hop of the *Route* header shall contain a SIP-URI of the obtained SCF address provided in clause c.2 with loose-routing specifier (i.e., ";lr"). The second and further hops of the *Route* header shall contain the given pre-existing route according to procedures as described in clause c.3.1. For a *REGISTER* request, pre-existing route is not provided.

c.3.3. Difference of address format retained by network

There may be a difference between a *Contact address* registered by a network and a *Contact address* set in a *REGISTER* request by a terminal. A terminal must be aware of it when verifying the *Contact address* URI.

- A URI parameter unrecognized by a network may not be retained.
- A *Contact address* may be retained in the format specifying no port number in a network, even if the default SIP port number (5060) is specified in the hostport part. The opposite could also be true that a *Contact address* may be retained in the format with the default port number (5060) in a network, even when the port number is not specified.

c.4. Refresh

In the case of receiving a *200 (OK)* response from a network indicating completion of registration or refresh, a terminal records the *Contact address* requested by the *REGISTER* request, and the retention period (*Z s*) returned by the *expires* parameter or in the *Expires* header field in the response.

Refresh interval (*T s*) MUST be set so that it does not exceed the retention period (*Z s*) and it does not cause frequent *REGISTER* request submissions. For example, setting the interval to a certain percentage of the retention period (*Z s*) is a good idea. The interval must be shorter than the value of retention period (*Z s*) minus Timer F (=32 s) specified in JF-IETF-RFC3261 [RFC3261] period in order to avoid expiration during resending the *REGISTER* request for refreshing. The refresh interval may be specified as a network option. [Annex Table j -24, Item 5]

c.5. Deletion

Considering that a terminal may experience a sudden power cutoff or a unexpected sequence during the shutdown process, the terminal should delete all *Contact addresses* that it registers after startup and before starting to register. A complete deletion should be performed by sending a *REGISTER* request which specifies * in *Contact address* and 0 in *Expires* header, in the event that the deletion of certain location information previously registered in some way cannot be guaranteed.

c.5.1. Considerations on terminal halt and IP address modification

A terminal should delete or update the *Contact address* registered in a network at times of rebooting, IP address modification, or application termination (in the case of softphone), etc.

c.6. Registration event

A network may provide a registration event (*reg* event) which notifies a terminal of its change of state from registered to unregistered as defined in JF-IETF-RFC3680[RFC3680]. [Annex Table j -24, Item 8]

In the case that a terminal desires to receive a notification of its change of registration state after registration is completed, it can be notified by using a registration event package function.

c.6.1. Subscription to registration event

In the case that a terminal desires to receive a notification of its change of state from registered to unregistered, it sets the registration event in a *SUBSCRIBE* request and requests to the network a subscription to the change notification of registration state (i.e., *reg* event). In the case that a network provides a change notification of registration state, it accepts the subscription, sets the information of registration state in a *NOTIFY* request, and notifies a terminal in accordance with the procedure defined in JF-IETF-RFC3265[RFC3265].

c.6.2. Notification of registration event

In the case that a terminal registration state is changed to unregistered, a network sets the unregistered state information in a *NOTIFY* request and notifies the terminal that subscribes to the registration event.

Annex d. SIP capabilities exchange

(This annex is a normative part of this standard.)

d.1. Overview

This annex describes procedures for capabilities exchange with SIP messages.

d.2. Available methods

This standard requires that methods of *INVITE*, *ACK*, *BYE*, and *CANCEL* are available in any *INVITE* sessions. However, the availability of other methods the network allows terminals to send is dynamically determined through a procedure of capabilities exchange. This clause and its subclauses describes the procedure.

d.2.1. UPDATE

A terminal asserts its capabilities to receive an *UPDATE* request by listing *UPDATE* in *Allow* header of initial *INVITE* request and *18x/2xx* responses to the *INVITE* request.

The terminal is allowed to send the *UPDATE* request in the case that the *Allow* header is set in the initial *INVITE* request or the *18x/2xx* response recently received, and *UPDATE* is listed in the header. In an early dialog, a *PRACK* transaction must be completed before sending the *UPDATE* request.

d.2.2. PRACK

In the case that a *Require* header is set in a *1xx* response (excluding *100 (Trying)*) received, and *100rel* is listed in the header, the terminal sends a *PRACK* to this response.

d.3. Extension function

This clause and its subclauses describe the procedure for capabilities exchange to judge whether to be able to use extension function.

d.3.1. Session timer function (timer)

A terminal sets *timer* in a *Supported* header when sending an *INVITE* request and an *UPDATE* request, and by doing so asserts to a network that it supports the function (A *Require* header must not be set to assert the *timer* in the *INVITE* request and the *UPDATE* request).

d.3.2. Provisional response reliability function (100rel)

A terminal asserts its support of this function by listing *100rel* in a *Supported* header when sending an *INVITE* request (A *Require* header must not be set to assert the *100rel* in the *INVITE* request).

In the case that the terminal receives a *1xx* response (excluding *100 (Trying)*) to the *INVITE* request sent and the response contains *100rel* in *Require* header, the terminal enables the *100rel* extension function only for this response, and sends a *PRACK* request.

Annex e. SDP and media handling

(This annex is a normative part of this standard.)

e.1. Overview

This annex supplements JF-IETF-RFC4566[RFC4566] and JF-IETF-RFC3264[RFC3264], and describes the procedure of media establishment and media change using SDP.

e.2. Judging a media change request

e.2.1. Receiving SDP

In the case that a terminal receives a re-*INVITE* or a *UPDATE* request including SDP, the terminal determines the request means a media change only when the *sess-version* value in *o=* line of the SDP is different from that of the SDP received as either offer or answer in the previous media establishment/change.

In the case that the terminal cannot perform the requested media change, it returns a *488 (Not Acceptable Here)* response, but it will not terminate the existing session. Whether the existing session would be terminated or not is left to the judgment of the terminal which requested a media change.

e.2.2. Sending SDP

In the case that an offer is made which lists multiple codecs (offer using RTP as media and listing several payload types in the *fmt* part of *m=* line), only part of the codecs are selected in the answer. In the case that this terminal sends afterwards a re-*INVITE* or *UPDATE* request which does not request a media change such as session refresh, it does not change the *sess-version* value in *o=* line as specified in section 7.4 of JF-IETF-RFC4028[RFC4028], nor change the content of SDP excluding *sess-version* as specified in section 8 of JF-IETF-RFC3264[RFC3264] accordingly. In the case that a session refresh is performed using an *UPDATE* request, it is recommended not to use SDP, in accordance with section 7.4 of JF-IETF-RFC4028[RFC4028].

e.3. Payload type

In the case that the media is RTP and a payload type number is statically assigned to the codec in JF-IETF-STD65[RFC3551], the assigned number is used in the *fmt* part of *m=* line. For example, in the case of G.711 μ -law, 0 is used in the *fmt* part.

In the case that a dynamic payload type number is specified due to the specifications of the codec, and the codec is selected as answer, the specified number in the offer is set to *m=* line of answer.

Note that a network may specify the maximum number of codecs that can be set in the *fmt* part of *m=* line. [Annex Table j -21, Item 3]

e.4. Fallback procedure

e.4.1. IP version incompatibility

A terminal should return a *488 (Not Acceptable Here)* response which includes a *Warning* header whose *warn-code* is *300 (Incompatible network protocol)* or *301 (Incompatible network address formats)* when it received an initial *INVITE* and determined that the requested IPv6 communication is not possible.

A terminal may receive a *488 (Not Acceptable Here)* response which includes a *Warning* header whose *warn-code* is *300 (Incompatible network protocol)* or *301 (Incompatible network address formats)* to the initial *INVITE* request it sent. In the case of receiving the above response to the session initiation with IPv6, the terminal interprets that communication using IPv6 is not possible and may try fallback with IPv4. However, further session initiation is not conducted even if it receives a *488* response to its fallback call.

e.4.2. Media type incompatibility

If no acceptable media type is set in the received SDP, a terminal returns a *488 (Not Acceptable Here)* response. The terminal sets *304 (Media type not available)* as *warn-code* in a *Warning* header of the *488* response.

Annex f. Congestion prevention and control

(This annex is a normative part of this standard.)

f.1. Overview

This annex describes behaviours that a network and a terminal should follow in order to prevent or control congestion.

f.2. Considerations on congestion control at time of registration

When a network requires terminal registration (*REGISTER*) at the UNI, all the users in this network are bound to send *REGISTER* requests regularly, which generates a load on the network to constantly process a multitude of messages. Therefore, considerations are necessary on the terminal behaviour so that it will not generate unnecessary loads on the network at time of registration.

f.2.1. Actions on receiving an error response

After sending a *REGISTER* request, a terminal may receive an error response that includes a *Retry-After* header (a *4xx*-response: in JF-IETF-RFC3261 [RFC3261], *404 (Not Found)* response, *413 (Request Entity Too Large)* response, *480 (Temporarily Unavailable)* response, *486 (Busy Here)* response, *500 (Server Internal Error)* response, *503 (Service Unavailable)* response, *600 (Busy Everywhere)* response, and a *603 (Decline)* response). In such a situation, the network may have some kind of problems such as congestion. Therefore, to avoid any further congestion, terminal registration is retried after the time interval specified in the *Retry-After* header (Note that an error response may be received again even when resending the *REGISTER* request after the specified time).

In the case that an error response is received without a *Retry-After* header, terminal registration is retried after an appropriate period of time (except on receiving a *401 (Unauthorized)* response) for the same reason.

f.2.2. Actions on receiving no response

A terminal may not be able to receive a response to a *REGISTER* request sent due to the retransmission timeout of SIP messages. An error may also occur in a layer below the SIP application layer (e.g., ICMP error notification). In such a situation, the terminal retries registration after an appropriate period of time. [Annex Table j -24, Item 7]

f.2.3. Considerations on registering multiple Contact addresses

Considerations should be given so that a terminal does not send a series of *REGISTER* requests in a short time in order to prevent unnecessary loads on a network triggered by the terminal registration behavior, in such cases where one terminal manages multiple AoRs, it needs to register multiple *Contact addresses* in the network, and consequently it sends multiple *REGISTER* requests, etc.

f.2.4. User name or password error

In the case that a terminal receives a *401 (Unauthorized)* response from a network after sending a *REGISTER* request containing an *Authorization* header, it should refrain from retrying registration using the same user name and password (excluding the case in which the value of the *stale* parameter in the *WWW-Authenticate* header is *TRUE*) so as to avoid the submission of unnecessary *REGISTER* requests.

f.2.5. Re-registration at the occurrence of temporary faults

If a terminal detects that it cannot send or receive SIP messages for some reason but it returns later to a state in which it can, it should immediately update registration or re-registration regardless of the change of its *Contact address* or registration retention period.

However, to avoid network congestion due to simultaneous registration behaviours caused by simultaneous terminal recoveries following a wide-area failure in the access network, and to avoid unnecessary repetition of terminal

registration behaviours due to intermittent temporary faults, the submission of *REGISTER* requests following fault recovery is made only at statistically uniform time intervals within an appropriate period of time. The network may specify a period of interval to resend the *REGISTER* request in the case that the network gives no reply. [Annex Table j -24, Item 7]

f.3. Considerations on congestion control when originating a call

The congestion may worsen if terminals attempts to make more calls (sending of requests outside existing dialogs except for *REGISTER*) to a network which already experiences congestion and call loss. Therefore, this clause and its subclauses describe a series of procedures so that in the case of congestion, the network notifies the terminal of the congestion state, the terminal notifies the user of the information notified by the network, and by doing so, the network notifies the user of the congestion state and attempts to control and prevent the user from redialing.

This clause and its subclauses also describe call retrial conditions so that congestion is not caused by a terminal's unlimited call retrials on receiving an error response when the call is made.

f.3.1. Congestion notification

This clause and its subclauses describe the error response format of congestion notification from the network, and required actions for terminals on receiving the notification.

f.3.1.1. Notification to a terminal from a network

In the case that a network cannot provide service to any request from a terminal due to congestion, etc., a *503 (Service Unavailable)* response is sent including a *Reason* header (*protocol* is *Q.850* and *protocol-cause* is *42: switching equipment congestion*) to a request from the terminal, which means that the network cannot provide service. The network never sends to the terminal the response including the *Reason* header (*protocol* is *Q.850* and *protocol-cause* is *42*) due to a cause other than congestion.

Notification of additional information indicated in clause f.3.2.1 may be performed along with congestion notification described in this clause.

f.3.1.2. Notification from a terminal to a user

In the case that a terminal receives a *503 (Service Unavailable)* response in which a *Reason* [RFC3326] header (*protocol* is *Q.850* and *protocol-cause* is *42: switching equipment congestion*) is set, it recognizes that a network cannot provide service to any request due to congestion, etc., and then performs visible indication to notify a user of the situation, or audible sound generation, such as a guidance to notify congestion or a signal tone to indicate congestion built into the terminal. Subsequent automatic behaviour, such as automatic call retrial, must not be performed.

In the case that additional information notification indicated in clause f.3.2.1 is performed at the same time, display of additional information indicated in clause f.3.2.1 is prioritized.

f.3.2. Additional information notification

This clause and its subclauses describe a procedure to notify a terminal of additional information from a network using a *Warning* header.

f.3.2.1. Notification from a network to a terminal

In the case that a network desires to provide additional information to a user when an error occurs, etc., it can notify a terminal of the information by including a *Warning* header in a response message sent back to the terminal, setting *399 (Miscellaneous warning)* as *warn-code*, and listing given text information in *warn-text*. The network must not send to the terminal the response in which the *Warning* header is set with *warn-code* *399*, excluding the case that the information intended to be notified to the user is included.